

REMARKS

Claims 1-8 have been examined with all claims rejected based on prior art. More specifically, claims 1-5 and 8 remain rejected under 35 USC 102(e) as being anticipated by Kash et al. (U.S. Patent No. 6,515,304; hereinafter "Kash"), and claims 6, 7, 9, and 10 are rejected under 35 USC 103(a) as being unpatentable over Kash in view of Klughart et al. (U.S. Patent No. 6,396,137; hereinafter "Klughart"). Applicant respectfully traverses this rejection for the reasons set forth below.

The claimed invention is concerned with the prevention of unauthorized external access to the operation of an integrated digital circuit. More specifically, the invention is concerned with counter-measures against so-called sidechannel attacks, which are performed by unauthorized parties for analyzing integrated digital circuits, for example, for analyzing coding algorithms performed by cryptocoprocessors.

Typically, integrated circuits are implemented as synchronous circuits, which operate on the basis of a clock signal. It is a standard approach in the prior art to introduce random wait states into the operation of such synchronous circuits to thus randomly delay timing of operation of such synchronous circuits. In a typical approach, an external clock is internally randomly delayed within the synchronous circuit to thus randomly postpone the occurrence of the internal operations along with the random delay of the clock to thus make it more difficult for unauthorized persons to analyze the internal operations.

The Examiner considers Kash's integrated circuit 1702 (see Fig. 6) to be an "asynchronous circuit." In this connection, he misinterprets page 2, lines 5-8, of the application in such a manner that, in the Examiner's opinion, an "asynchronous" integrated circuit is an integrated circuit that operates in an asynchronous manner. This definition is meaningless and does not correctly define the technical difference between a synchronous circuit and an asynchronous circuit. The term "asynchronous circuit" has a clear technical meaning to one of ordinary skill in the present field. As evidence, attached is the definition of an asynchronous circuit, as provided by Wikipedia. An

asynchronous circuit is a circuit, which is not governed by any clock signal. An asynchronous circuit is contrasted with a synchronous circuit, which operates according to clock timing signals.

Kash's circuit shown in Fig. 6 operates based on an external clock, which is randomly delayed in order to generate a jittered internal chip clock, which forms the basis of the operation of the internal clocked circuit 1712. By definition, Kash is concerned with a synchronous circuit, namely with a circuit which operates according to clock timing signals, although the internal clock timing signal is somewhat jittered or randomly delayed. However, the jitter or the random delay of the clock does not change the nature of the circuit, namely to be a synchronous circuit. It operates in synchronism with the jittered or randomly delayed internal clock.

Kash discloses in connection with Fig. 6 an integrated circuit having a synchronous clocked circuit 1712 operated in synchronism with a jittered or randomly delayed internal chip clock. With regard to the feature concerning the variation of the electric voltage supply, the Examiner refers to column 3, line 66, to column 4, line 3, of the reference. This section of the reference has nothing to do with the integrated circuit discussed in connection with Fig. 6. Rather, it refers to a typical technology used for facilitating the non-destructive reverse engineering of a circuit by monitoring the modulation of a reflected light beam by parts of active elements or devices in the integrated circuit (see column 3, lines 51-55). A time varying voltage across an interface in the integrated circuit produces a time-varying modulating of reflectivity from the interface that can be measured and used to obtain information about the time varying voltage (see column 3, line 66, through column 4, line 3). This is only the measurement technique for analyzing the operation of internal parts of an integrated circuit by a reflected light beam and has nothing to do with the variation of a supply voltage of the circuit. Thus, the Examiner's implicit argument that the time-varying of the electrical voltage supply is taught by column 3, line 66, through column 4, line 3, of the reference is obviously based on a technical misunderstanding on the Examiner's part.

Klughart also does not deal with any asynchronous circuits. Rather, this reference is concerned with measures which establish additional security against reverse engineering performed by third parties (see column 34, lines 42-48). Klughart teaches arranging layers of metal and

specific semiconductor layers above switches and regulators in integrated circuits to thus prevent unauthorized access by third parties to the operation of these switches or regulators (see column 34, lines 49-64).

The Examiner's allegations that Klughart discloses an asynchronous circuit are not supported by the disclosure of the reference. The Examiner refers to column 16, lines 49-53. However, this section of the description does not deal with asynchronous circuits.

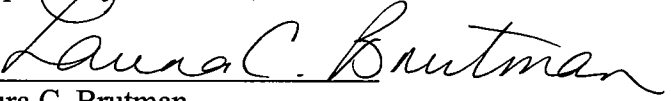
The Examiner further refers to column 37, lines 30-35. This section refers to a switching regulator/power converter which asynchronously modulates its pulse width or frequency, in order to compensate for changing load requirements. This is not an asynchronous circuit. As explained above, an asynchronous circuit is a circuit which is not governed by any clock signal. Such a circuit is not disclosed by Klughart. Moreover, Klughart does not teach or suggest varying the supply voltage of any asynchronous circuit.

In view of the above amendment, Applicant believes the pending application is in condition for allowance.

In the event a fee is required or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge the underpayment to Deposit Account No. 50-2215.

Dated: September 24, 2007

Respectfully submitted,

By 
Laura C. Brutman

Registration No.: 38,395
DICKSTEIN SHAPIRO LLP
1177 Avenue of the Americas
New York, New York 10036-2714
(212) 277-6500
Attorney for Applicant

Asynchronous circuit

From Wikipedia, the free encyclopedia

An **asynchronous circuit** is a circuit in which the parts are largely autonomous. They are not governed by a clock circuit or global clock signal, but instead need only wait for the signals that indicate completion of instructions and operations. These signals are specified by simple data transfer protocols. This digital logic design is contrasted with a synchronous circuit which operates according to clock timing signals.

Contents

- 1 Benefits
- 2 Applications
- 3 Theoretical Foundations
- 4 Quotations
- 5 See also

Benefits

Different classes of asynchronous circuitry offer different advantages. Below is a list of the advantages offered by Quasi Delay Insensitive Circuits, generally agreed to be the most "pure" form of asynchronous logic that retains computational universality. Less pure forms of asynchronous circuitry offer better performance at the cost of compromising one or more of these advantages.

- Robust handling of metastability of arbiters.
- Early Completion of a circuit when it is known that the inputs which have not yet arrived are irrelevant
- Possibly lower power consumption due to the fact that no transistor ever transitions unless it is performing useful computation (clock gating in synchronous designs is an imperfect approximation of this ideal). However, when using certain encodings, asynchronous circuits may require more area, which can result in increased power consumption if the underlying process has poor leakage properties (for example, deep submicron processes used prior to the introduction of high-K dielectrics).
- Freedom from the ever-worsening difficulties of distributing a high-fanout, timing-sensitive clock signal
- Better modularity and composability
- Far fewer assumptions about the manufacturing process are required (most assumptions are timing assumptions)
- Circuit speed is adapted on the fly to changing temperature and voltage conditions rather than being locked at the speed mandated by worst-case assumptions.
- Immunity to transistor-to-transistor variability in the manufacturing process, which is one of the most serious problems facing the semiconductor industry as dies shrink.
- Less severe electromagnetic interference. Synchronous circuits create a great deal of EMI in the frequency band at (or very near) their clock frequency; asynchronous circuits generate EMI patterns which are much more evenly spread across the spectrum.

Applications

ILLIAC II in 1962 was the first completely asynchronous, speed independent processor design.

DEC PDP-16 Register Transfer Modules (ca. 1973) allowed the experimenter to construct asynchronous, 16-bit processing elements. Delays for each module were fixed and based on the module's worst-case timing.

Caltech designed and manufactured the world's first fully Quasi Delay Insensitive processor. During demonstrations, the researchers amazed viewers by loading a simple program which ran in a tight loop, pulsing one of the output lines after each instruction. This output line was connected to an oscilloscope. When a cup of hot coffee was placed on the chip, the pulse rate (the effective "clock rate") naturally slowed down to adapt to the worsening performance of the heated transistors. When liquid nitrogen was poured on the chip, the instruction rate shot up with no additional intervention. Additionally, at lower temperatures, the voltage supplied to the chip could be safely increased, which also improved the instruction rate -- again, with no additional configuration.

In 2004, Epson manufactured the world's first flexible microprocessor, an 8-bit asynchronous chip. Synchronous flexible processors are slower, since bending the material on which a chip is fabricated causes wild and unpredictable variations in the delays of various transistors, for which worst case scenarios must be assumed everywhere and clock everything at worst case speed. The processor is intended for use in smart cards, whose chips are currently limited in size to those small enough that they can remain perfectly rigid.

Theoretical Foundations

Some have argued that Petri Nets are an attractive and powerful model for reasoning about asynchronous circuits. However Petri nets have been criticized by Carl Hewitt and others for their lack of physical realism (see Petri net#Subsequent models of concurrency). Subsequent to Petri nets other models of concurrency have been developed that can model asynchronous circuits including the Actor model and process calculi.

The term *asynchronous logic* is used to describe a variety of design styles, which use different assumptions about circuit properties. These vary from the bundled delay model - which uses 'conventional' data processing elements with completion indicated by a locally generated delay model - to delay-insensitive design - where arbitrary delays through circuit elements can be accommodated. The latter style tends to yield circuits which are larger and slower than synchronous (or bundled data) implementations, but which are insensitive to layout and parametric variations and are thus "correct by design."

Quotations

- "Having spent untold hours debugging digital designs, I can assure you that metastable behavior is a real problem, and every digital designer had better understand it" -- Bruce Nepple 1998-12-31
- "Clocks are an ever-increasing source of trouble. Most designs use a single clock source that drives perhaps dozens of chips. There's little doubt that the resulting long clock wire will be rife with reflections, destroying its shape. Unfortunately, most CPUs are quite sensitive to the shape and level of the clock." -- Jack Ganssle

See also

- An introduction to asynchronous circuit design by Davis and Nowick
- Asynchronous systems

- Asynchronous logic
- Synchronous circuit
- Universal asynchronous receiver transmitter
- null convention logic ([1]) "In September 2000, Theseus Logic released NCL08, an 8-bit microcontroller"
- The Red Star seems to be a version of the MIPS R3000 implemented in asynchronous (clockless) logic
- It is rumored that "Alain Martin, the first person to fab an asynchronous microprocessor".
- The Amulet microprocessors were asynchronous ARMs, built in the 1990s
- The N-Protocol developed by Navarre AsyncArt, first fully commercial asynchronous design methodology optimized for conventional FPGAs.
- PGPSALM- An asynchronous implementation of the 6502 microprocessor

Retrieved from "http://en.wikipedia.org/wiki/Asynchronous_circuit"

Categories: All articles with unsourced statements | Articles with unsourced statements since February 2007 | Electrical circuits | Parallel computing

- This page was last modified 06:47, 3 August 2007.
- All text is available under the terms of the GNU Free Documentation License. (See **Copyrights** for details.)
Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a US-registered 501 (c)(3) tax-deductible nonprofit charity.